UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/822,927	04/12/2004	Eliot Lear	50325-0864	4441

29989 7590 08/31/2009

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
08/31/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/822,927	LEAR, ELIOT	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-21,23-25,27-29,31,32,34-37,39-42 and 44-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-21,23-25,27-29,31,32,34-37,39-42 and 44-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.
Applicant's submission filed on 6-18-2009 has been entered.

2. Claims **1, 4 - 21, 23 - 25, 27 - 29, 31, 32, 34 - 37, 39 - 42, 44 - 47** are pending. Claims **1, 8, 12, 18, 20, 21, 24, 25, 28, 29, 32** have been amended. Claims **2, 3, 22, 26, 30, 33, 38, 43** have been cancelled. Claims **1, 8, 18, 21, 25, 29** are independent. This application was filed on 4-12-2004.

Response to Arguments

3. Applicant's arguments have been fully considered but they were not persuasive.

3.1 The previous 112 rejection has been withdrawn due to Remarks.

3.2 Applicant argues that the referenced prior art does not disclose, *signature for first portion and signature for second portion. (Remarks Pages 18, 19)*

Mott prior art discloses hash generation for a portion of a message and a hash generated for a second (or next) portion of a message. (see Mott col 19, ll 18-36:

computes a secure hash for each n seconds the portion of program data (message data))

3.3 Applicant argues that the referenced prior art does not disclose, *a number of required signatures. (Remarks Pages 19, 20)*

Kinnis prior art discloses a parameter for a number of signatures. (see Kinnis col. 8, lines 50-56: file attributes may include the number of times the file has been signed)

3.4 Applicant argues that the referenced prior art does not disclose, *collective authority. (Remarks Pages 20 - 22)*

Sudia prior art discloses a collective authority concept. (see Sudia paragraph [0250], lines 6-16: if multiple delegates need to authorize the user's card, they may sequentially sign the request)

3.5 Applicant argues that the referenced prior art does not disclose, *a valid time period. (Remarks Pages 25, 26)*

Sudia prior art discloses a valid time period for the application of a digital signature. (see Sudia paragraph [0249], lines 1-14: time limit (expiration period) for certificate (key information))

3.6 Applicant argues *the dependent claims. (Remarks Page 27)*

Arguments for dependent claims are based upon above arguments for independent claims. The successful responses to arguments for independent claims also successfully respond to the current arguments against the dependent claims.

3.7 Bosler prior art discloses a network management system for the management of interconnected network entities. Bosler prior art discloses a public key infrastructure and digital signature mechanism as an authentication mechanism. And, the Bosler prior art discloses the completion of authentication before configuration commands or directives are processed by a second management. The Bosler prior art discloses the authentication or verification of a digital signature (hash). (see Bosler paragraph [0078], lines 1-15: if first hash matches second hash, then authentication successful)

Bosler prior art discloses that digital signature information used for authentication is transferred between network connected nodes. (see Bosler paragraph [0058], lines 21-28: receive security information with directive (i.e. command, management message); paragraph [0058], lines 5-14: digital signature authentication; paragraph [0069], lines 1-5: apply directives or commands after authentication)

Bosler prior art discloses the usage of digital signatures for authentication or verification. The specification specified "combined authority" is equivalent to a determination of whether an entity is authorized. Bosler prior art discloses whether an entity is authorized to make a configuration change. (see Bosler paragraph [0078],lines 1-15: if both hash values match, then, the message (configuration directive) is authentication (verified, authorized) and can be processed) And, the Kinnis prior art discloses the usage of more than one digital signature in authentication. Each additional digital signature is verified or authorized (equivalent to combined authority). (see Kinnis col. 10, lines 38-67: authentication (verification) of multiple signatures)

And, the Sudia prior art discloses an expiration time period for digital certificates.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **1, 4 - 7, 20, 21, 23 - 25, 27 - 29, 31, 32, 34 - 37, 39 - 42, 44 - 47** are rejected under 35 U.S.C. 103 (a) as being unpatentable over **Bosler et al.** (US PGPUB No. **20050010757**) in view of **Kinnis et al.** (US Patent No. **6,959,382**) and further in view of **Sudia et al.** (US PGPUB No. **20020013898**) and **Mott et al.** (US Patent No. **6,170,060**).

With Regards to Claims 1, 21, 25, Bosler discloses a method, a computer-readable volatile or non-volatile medium storing one or more sequences of instructions, apparatus comprising the computer implemented steps of:

a) receiving trust information defining one or more trusted signatories; (see Bosler paragraph [0058], lines 5-7: public/private key pairs; paragraph [0060], lines 1-6: CAs (i.e. trusted signatories) distributing or granting certificates, received by user)

Furthermore, Bosler discloses the following:

c) receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and one or more digital signatures of the hostname and configuration directives; (see Bosler paragraph [0058], lines 5-14: management (i.e. configuration) information transferred between manager and client, digital signature verification required)

d) wherein the configuration information includes the particular configuration directive; (see Bosler paragraph [0058], lines 21-28: receive security information with directive (i.e. command, management message)) (see Bosler paragraph [0058], lines 21-28: receive (transfer) security information with directives (i.e. command, management message));

f) attempting to verify the one or more digital signatures based on the trust information; (see Bosler paragraph [0008], lines 7-13: verification digital signature based on certificates received from CA (i.e. trust information))

h) applying the configuration directives to the host network element only when the two of more digital signatures are verified successfully; (see Bosler paragraph [0057], lines 29-33: utilize directives or commands after digital signature verification)

i) wherein applying the configuration directives comprises applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals. (see Bosler paragraph [0058], lines 21-28: receive security information with directive (i.e. command,

management message); digital signature information (associated principals information); paragraph [0058], lines 5-14: digital signature authentication; paragraph [0069], lines 1-5: apply directives or commands after authentication; there is no disclosure for a parameter to indicate the number of required signatures by the required principals)

j) wherein the steps of the method are performed by the host network element. (Bosler paragraph [0057], lines 23-28: network management system; distributed system; management server and agents on managed nodes)

Furthermore, Bosler discloses wherein verifying that one or more digital signatures, from the one or more digital signatures, are valid and that two or more principals respectively associated with the two or more digital signatures have authority to perform the configuration directives on the host network element; (see Bosler paragraph [0008], lines 7-13; paragraph [0078], lines 7-15: management information, verify digital signature)

Furthermore, Bosler discloses receiving, in association with a particular configuration directive, security information. (see Bosler paragraph [0058], lines 21-28: receive security information with directive (i.e. command, management message); paragraph [0058], lines 5-14: digital signature authentication)

Bosler does not specifically disclose defining a number of required signatures and verifying two or more digital signatures.

However, Kinnis discloses:

b) defining a number of required signatures and required principals; (see Kinnis col. 8, lines 50-56: file attributes may include the number of times the file has been signed and certificates)

g) verifying that two or more digital signatures are valid. (see Kinnis col. 10, lines 38-67: verify multiple signature (first, second) authenticated; col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes; col. 4, lines 25-27: content of any type can be protected with digital signature; col. 4, lines 31-34: certificate from Certificate Authority (CA))

It would have been obvious to one of ordinary skill in the art to modify Bosler for defining a number of required signatures and utilizing multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

Bosler-Kinnis does not specifically disclose collective authority.
However, Sudia discloses collective authority. (see Sudia paragraph [0250], lines 6-16: if multiple delegates need to authorize the user's card, they may sequentially sign the request)

It would have been obvious to one of ordinary skill in the art to modify Bosler-

Kinnis for collective authority as taught by Sudia. One of ordinary skill in the art would have been motivated to employ the teachings of Sudia to provide a robust and easy-to-use mechanism in which authorizing agents can temporarily delegate their authorizing capability based on a time period. (see Sudia paragraph [0011], lines 1-4)

Bosler-Kinnis-Sudia does not specifically disclose a signature for a first portion and a second portion of a message.

However, Mott discloses:

d) wherein the two or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, and a second digital signature of a second portion of the one or more configuration directives by a second user; (see Mott col 19, ll 18-36: computes a secure hash for each n seconds the portion of program data (message data))

It would have been obvious to one of ordinary skill in the art to modify Bosler-Kinnis-Sudia a signature for a first portion and a second portion of a message as taught by Mott. One of ordinary skill in the art would have been motivated to employ the teachings of Mott to take advantage of the new possibilities for personalized access for usage of large amounts of information based on the advances in compression of digital data and expansion of storage capacities. (Mott col 1, ll 12-20)

With Regards to Claim 4, Bosler discloses a method as recited in Claim 1,

wherein applying the particular configuration directive comprises applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures. (see Bosler paragraph [0058], lines 5-14: digital signature authentication; paragraph [0069], lines 1-5: apply directives or commands after authentication)

With Regards to Claim 5, Bosler discloses a method as recited in claim 1, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures are stored on the host. (see Bosler paragraph [0073], lines 4-7: security information stored in central location (i.e. host system), (i.e. option, each individual system or host))

Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools.

(see Kinnis col. 2, lines 20-26)

With Regards to Claim 6, Bosler discloses a method as recited in Claim 1, wherein the digital signatures use public key cryptography, wherein public keys for the digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the digital signatures. (see Bosler paragraph [0007], lines 6-8: public key cryptography authentication; paragraph [0073], lines 4-7; paragraph [0060], lines 1-6: security information stored in central location or in each individual system or host, certification server (i.e. key server))

Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

With Regards to Claim 7, Bosler discloses a method as recited in Claim 1, wherein the

digital signatures use public key cryptography, and wherein public keys for the digital signatures are received in a digital certificate and extracted from the digital certificate as part of attempting to validate the digital signatures. (see Bosler paragraph [0058], lines 5-7: public/private key pair; paragraph [0060], lines 1-6: Certificate Authority (CA) , public key certificate; paragraph [0008], lines 7-13: verification (i.e. validation) with digital signature)

Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

With Regards to Claim 20, Bosler discloses a method, as recited in any of Claim 18, wherein the digital signatures comprise a first digital signature of a portion of the one or more configuration directives by a first user, a second digital signature of a portion of the one or more configuration directives by a second user, and a third digital signature

by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature. (see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)

Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

Bosler does not specifically disclose a signature for a first portion and a second portion of a message.

However, Mott discloses a first digital signature of a first portion of the one or more configuration directives by a first user, a second digital signature of a second portion of the one or more configuration directives by a second user. (see Mott col 19, ll 18-36: computes a secure hash for each n seconds the portion of program data (message data))

It would have been obvious to one of ordinary skill in the art to modify Bosler a signature for a first portion and a second portion of a message as taught by Mott. One of ordinary skill in the art would have been motivated to employ the teachings of Mott to take advantage of the new possibilities for personalized access for usage of large amounts of information based on the advances in compression of digital data and expansion of storage capacities. (Mott col 1, ll 12-20)

With Regards to Claims 23, 31, Bosler discloses a computer-readable volatile or non-volatile medium, apparatus as recited in any of Claims 21, 29, wherein the digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature. (see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)

Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art

would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

With Regards to Claims 24, 32, Bosler discloses a method, computer-readable volatile or non-volatile medium, apparatus as recited in any of Claims 21, 29, wherein the digital signatures further comprise a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature. (see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)
Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

With Regards to Claim 27, Bosler discloses an apparatus as recited in Claim 25, wherein the digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature. (see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)
Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

With Regards to Claim 28, Bosler discloses an apparatus as recited in Claim 25, wherein the digital signatures further comprise a third digital signature by a third user, wherein the third digital signature is applied to a resultant of the first digital signature and the second digital signature. (see Bosler paragraph [0078], lines 7-15: comparison

(i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)

With Regards to Claim 29, Bosler discloses an apparatus for verifying configuration changes for network devices using digital signatures, comprising: a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a) a processor; (see Bosler paragraph [0067], lines 4-8: processor)

Furthermore, Bosler disclose the following:

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

b) receiving trust information defining one or more trusted signatories; (see Bosler paragraph [0058], lines 5-7: public/private key pairs; paragraph [0060], lines 1-6: CAs (i.e. trusted signatories) distributing or granting certificates, received by user)

c) receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, and one or more digital signatures of the hostname and configuration directives; (see Bosler paragraph [0058], lines 5-14: management (i.e. configuration) information transferred between manager and client, digital signature verification required)

f) verifying that two or more digital signatures, from the one or more digital signatures, are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the

configuration directives on the host network element; (see Bosler paragraph [0008], lines 7-13: verify digital signature)

g) applying the configuration directives to the home network element only when the one or more digital signatures are verified successfully. (see Bosler paragraph [0058], lines 5-14; paragraph [0069], lines 1-5: signature verification, process directive)

Furthermore, Bosler discloses wherein verifying that one or more digital signatures, from the one or more digital signatures, are valid and that two or more principals respectively associated with the two or more digital signatures have authority to perform the configuration directives on the host network element; (see Bosler paragraph [0008], lines 7-13; paragraph [0078], lines 7-15: management information, verify digital signature)

Furthermore, Bosler discloses the configuration information includes the particular configuration directive. (Bosler paragraph [0057], lines 1-5: management messages (directives) exchanged during a session between management server and managed nodes)

Bosler does not specifically disclose two or more digital signatures.

However, Kinnis discloses:

e) verifying that two or more digital signatures, from the one or more digital signatures, are valid; (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added; col. 3, lines 28-

30: used for authentication purposes; col. 4, lines 25-27: content of any type can be protected with digital signature; col. 4, lines 31-34: certificate from Certificate Authority (CA))

It would have been obvious to one of ordinary skill in the art to modify Bosler to enable the capability to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

Bosler-Kinnis does not specifically disclose collective authority.
However, Sudia discloses collective authority. (see Sudia paragraph [0250], lines 6-16: if multiple delegates need to authorize the user's card, they may sequentially sign the request)

It would have been obvious to one of ordinary skill in the art to modify Bosler-Kinnis for collective authority as taught by Sudia. One of ordinary skill in the art would have been motivated to employ the teachings of Sudia to provide a robust and easy-to-use mechanism in which authorizing agents can temporarily delegate their authorizing capability based on a time period. (see Sudia paragraph [0011], lines 1-4)

Bosler-Kinnis-Sudia does not specifically disclose a signature for a first portion and a second portion of a message.
However, Mott discloses:

d) wherein the two or more digital signatures comprise a first digital signature of a first portion of the one or more configuration directives by a first user, and a second digital signature of a second portion of the one or more configuration directives by a second user; (see Mott col 19, ll 18-36: computes a secure hash for each n seconds the portion of program data (message data))

It would have been obvious to one of ordinary skill in the art to modify Bosler-Kinnis-Sudia for a signature for a first portion and a second portion of a message as taught by Mott. One of ordinary skill in the art would have been motivated to employ the teachings of Mott to take advantage of the new possibilities for personalized access for usage of large amounts of information based on the advances in compression of digital data and expansion of storage capacities. (Mott col 1, ll 12-20)

With Regards to Claims 34, 39, 44, Bosler discloses a computer-readable volatile or non-volatile medium, apparatus as recited in Claims 21, 25, 29, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of: receiving, in association with a particular configuration directive, security information; applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures. (see Bosler paragraph [0058], lines 5-7: public/private key pair; paragraph [0060], lines 1-6: Certificate Authority (CA) , public key certificate; paragraph [0008], lines 7-13;

paragraph [0078], lines 7-15: verification (i.e. validation) with digital signature(s); paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Bosler does not specifically disclose a number of required signatures.

However, Kinnis discloses defining a number of required signatures and required principals. (see Kinnis col. 8, lines 50-56: file attributes may include the number of times the file has been signed and certificates)

It would have been obvious to one of ordinary skill in the art to modify Bosler for defining a number of required signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

With Regards to Claims 35, 40, 45, Bosler discloses a computer-readable volatile or non-volatile medium, apparatus as recited in Claims 21, 25, 29, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures are stored on the host network element. (see Bosler paragraph [0073], lines 4-7: security information stored in central location (i.e. host system), (i.e. option, each individual system or host); paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Bosler does not specifically disclose the usage of two or more digital signatures.

However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24:

first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

With Regards to Claims 36, 41, 46, Bosler discloses a computer-readable volatile or non-volatile medium, apparatus as recited in Claims 21, 25, 29, wherein the digital signatures use public key cryptography, wherein public keys for the digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the digital signatures. (see Bosler paragraph [0007], lines 6-8: public key cryptography authentication; paragraph [0073], lines 4-7; paragraph [0060], lines 1-6: security information stored in central location or in each individual system or host, certification server (i.e. key server); paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software, implementation means)

Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added

(integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

With Regards to Claims 37, 42, 47, Bosler discloses a computer-readable volatile or non-volatile medium, apparatus as recited in Claims 21, 25, 29, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures received in a digital certificate and extracted from the digital certificate as part of attempting to validate the digital signatures. (see Bosler paragraph [0058], lines 5-7: public/private key pair; paragraph [0060], lines 1-6: Certificate Authority (CA) , public key certificate; paragraph [0008], lines 7-13: verification (i.e. validation) with digital signature; paragraph [0057], lines 23-28; paragraph [0066], lines 1-4: software) Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30:

used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

6. Claims **8 - 19** are rejected under 35 U.S.C. 103 (a) as being unpatentable over **Bosler-Kinnis** and further in view of **Sudia**.

With Regards to Claim 8, Bosler discloses a method, comprising the computer implemented steps of:

a) receiving a public key for a user of the network devices; receiving trust information defining one or more trusted signatories; (see Bosler paragraph [0058], lines 5-7: public/private key pairs; paragraph [0060], lines 1-6: CAs (i.e. trusted signatories) distributing or granting certificates)

Furthermore, Bosler discloses the following:

b) receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives; (see Bosler paragraph [0071], lines 1-13; paragraph [0073], lines 77-22: time-based certificate, directive authentication)

g) wherein the steps of the method are performed by the host network element.

(Bosler paragraph [0057], lines 23-28: network management system; distributed system; management server and agents on managed nodes)

Furthermore, Bosler and Sudia disclose the following:

c) receiving configuration information comprising a hostname, one or more configuration directives for a host network element associated with the hostname, one or more digital signatures of the hostname and configuration directives, (see Bosler paragraph [0058], lines 5-14: management (i.e. configuration) information transferred between manager and client, digital signature verification required) and a date time value; (see Sudia paragraph [0249], lines 1-14: time limit (expiration period) for certificate (key information))

d) determining if the date time value is within the time period; (see Sudia paragraph [0249], lines 1-14: time limit (expiration period) for certificate (key information))-

e) determining if the one or more configuration directives have been previously received; (see Bosler paragraph [0069], lines 1-5: process configuration directive(s), commands) during the time period (see Sudia paragraph [0249], lines 1-14: time limit (expiration period) for certificate (key information)) and

f) only when the date time value is within the time period (see Bosler paragraph [0073], lines 17-22: time based certificate) and the one or more configuration directives have not been previously received during the time period, attempting to verify the one or more digital signatures based on the trust information, and applying the configuration directives to a network element only when the one or more digital signatures are verified successfully. (see Sudia paragraph [0249],

lines 1-14: time limit (expiration period) for certificate (key information))

It would have been obvious to one of ordinary skill in the art to modify Bosler to use a time period to limit usage of security information as taught by Sudia. One of ordinary skill in the art would have been motivated to employ the teachings of Sudia to provide a robust and easy-to-use mechanism in which authorizing agents can temporarily delegate their authorizing capability based on a time period. (see Sudia paragraph [0011], lines 1-4)

With Regards to Claims 9, 10, Bosler discloses a method as recited in Claim 8, wherein the step of determining if the one or more configuration directives have been previously received during the time period comprises the steps of

a) generating a secure hash of the one or more configuration directives; (see Bosler paragraph [0078], lines 3-15: generate secure hash value for authentication)
b) determining if the secure hash is found in non volatile memory. (see Bosler paragraph [0078], lines 3-15; paragraph [0067], lines 4-8: memory, workspace for data processing: memory (i.e. non-volatile))

With Regards to Claim 11, Bosler discloses a method as recited in Claim 8, further comprising the step of storing the secure hash in non volatile memory, and the one or more configuration directives have not been previously received during the time period. (see Bosler paragraph [0067], lines 4-8: memory, workspace for data processing; paragraph [0078], lines 3-15: hash (i.e. digest) values utilized for authentication)

Bosler does not specifically disclose an association with an expiration value, and when the date time value is within a time period.

However, Sudia discloses wherein association with an expiration value, when the date time value is within the time period. (see Sudia paragraph [0249], lines 1-14: time limit (expiration period) for certificate (key information))

It would have been obvious to one of ordinary skill in the art to modify Bosler to use a time period to limit usage of the security information as taught by Sudia. One of ordinary skill in the art would have been motivated to employ the teachings of Sudia to provide a robust and easy-to-use mechanism in which authorizing agents can temporarily delegate their authorizing capability based on a time period. (see Sudia paragraph [0011], lines 1-4)

With Regards to Claim 12, Bosler discloses a method as recited in Claim 8, further comprising the steps of verifying that the one or more digital signatures is valid and that one or more principals respectively associated with the digital signatures have collective authority to perform the directives on the host network element. (see Bosler paragraph [0058], lines 5-14: mutual authentication required before directive(s) or command(s) implemented)

With Regards to Claims 13, 14, Bosler discloses a method as recited in Claim 8, further comprising the steps of

a) receiving, in association with a particular configuration directive, security

information; (see Bosler paragraph [0058], lines 21-28: key, security information received with directive or command)

Furthermore, Bosler discloses:

b) applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals and only upon successively validating all required signatures. (see Bosler paragraph [0058], lines 5-14; paragraph [0069], lines 1-5: validate digital signature, process directive or command)

Bosler does not specifically disclose a number of required signatures. However, Kinnis discloses defining a number of required signatures and required principals. (see Kinnis col. 8, lines 50-56: file attributes may include the number of times the file has been signed and certificates)

It would have been obvious to one of ordinary skill in the art to modify Bosler for defining a number of required signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

With Regards to Claim 15, Bosler discloses a method as recited in claim 1, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures are stored on the host. (see Bosler paragraph [0073], lines 4-7: security information stored in central location (i.e. host system), (i.e. option, each

individual system or host))

Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

With Regards to Claim 16, Bosler discloses a method as recited in Claim 1, wherein the digital signatures use public key cryptography, wherein public keys for the digital signatures are stored on a key server and retrieved from the key server as part of attempting to validate the digital signatures. (see Bosler paragraph [0007], lines 6-8: public key cryptography authentication; paragraph [0073], lines 4-7; paragraph [0060], lines 1-6: security information stored in central location or in each individual system or host, certification server (i.e. key server))

Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24:

first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

With Regards to Claim 17, Bosler discloses a method as recited in Claim 1, wherein the digital signatures use public key cryptography, and wherein public keys for the digital signatures are received in a digital certificate and extracted from the digital certificate as part of attempting to validate the digital signatures. (see Bosler paragraph [0058], lines 5-7: public/private key pair; paragraph [0060], lines 1-6: Certificate Authority (CA) , public key certificate; paragraph [0008], lines 7-13: verification (i.e. validation) with digital signature)

Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30:

used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

With Regards to Claim 18, Bosler discloses a method for verifying configuration changes for network devices using digital signatures, comprising the computer implemented steps of:

a) receiving a public key for a user of the network devices; (see Bosler paragraph [0058], lines 5-7: public/private key pairs; paragraph [0060], lines 1-6: CAs (i.e. trusted signatories) distributing or granting certificates (i.e. public key certificate), received by user)

Furthermore, Bosler discloses the following:

b) receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives to a specified network device; (see Bosler paragraph [0071], lines 1-13; paragraph [0073], lines 17-22: time based certificate)

c) receiving configuration information comprising a hostname, one or more configuration directives for the specified network device associated with the hostname, one or more digital signatures of the hostname and configuration

directives, and a date time value; (see Bosler paragraph [0058], lines 5-14: management (i.e. configuration) information transferred between manager and client, digital signature verification required)

e) determining if the one or more configuration directives have been previously received during the time period, by generating a secure hash of the one or more configuration directives and determining if the secure hash is found in memory; (see Bosler paragraph [0078], lines 3-15: hash (i.e. digest) utilized) and

performing the steps of:

g) attempting to verify the one or more digital signatures based on generating a secure hash of the one or more configuration directives using the public key and comparing the secure hash to the one or more digital signatures, and applying the configuration directives to the specified network device only when the one or more digital signatures are verified successfully. (see Bosler paragraph [0078], lines 3-15: hash generation, authentication)

h) wherein the steps of the method are performed by the specified network device.

g) wherein the steps of the method are performed by the host network element. (Bosler paragraph [0057], lines 23-28: network management system; distributed system; management server and agents on managed nodes)

And, Sudia discloses:

d) determining if the date time value is within the time period; (see Sudia paragraph [0249], lines 1-14: time limit (expiration period) for certificate (key information))

f) only when the date time value is within the time period and the one or more

configuration directives have not been previously received during the time period, (see Sudia paragraph [0249], lines 1-14: time limit (expiration period) for certificate (key information))

It would have been obvious to one of ordinary skill in the art to modify Bosler to use a time period to limit usage of the security information as taught by Sudia. One of ordinary skill in the art would have been motivated to employ the teachings of Sudia to provide a robust and easy-to-use mechanism in which authorizing agents can temporarily delegate their authorizing capability based on a time period. (see Sudia paragraph [0011], lines 1-4)

With Regards to Claim 19, Bosler discloses a method, as recited in any of Claims 18, wherein the digital signatures comprise a first digital signature of the one or more configuration directives by a first user, and a second digital signature by a second user, wherein the second digital signature is applied to a resultant of the first digital signature. (see Bosler paragraph [0078], lines 7-15: comparison (i.e. is applied) of resultant hashes (i.e. digest, digital signature) for authentication)

Bosler does not specifically disclose the usage of two or more digital signatures. However, Kinnis discloses two or more digital signatures. (see Kinnis col. 3, lines 3-24: first, second digital signatures for content, any number of signatures may be added (integrity of first signature maintained when second signature appended; only usage for digital signature is verification or authentication of an entity or user); col. 3, lines 28-30: used for authentication (verification) purposes)

It would have been obvious to one of ordinary skill in the art to modify Bosler to utilize multiple digital signatures as taught by Kinnis. One of ordinary skill in the art would have been motivated to employ the teachings of Kinnis to obtain certificates, keys, and generate digital signatures that may be stored independent of other tools. (see Kinnis col. 2, lines 20-26)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
August 17, 2009